Full Paper

A FUZZY LOGIC BASED PROACTIVE MAINTENANCE SCHEDULING ON COMMUNICATION NETWORKS

E. A. Olajubu
Department of Computer Science & Engineering
Faculty of Technology
Obafemi Awolowo University, Nigeria
emmolajubu@oauife.edu.ng

ABSTRACT

This paper presents a fuzzy logic methodology for scheduling predictive maintenance on communication networks. Lightweight agents were used to monitor and collect network elements status information at intervals of time which indicated the condition of each component, and the overall health of the network element. Data analyzer used to process status information of each component data was model with fuzzy logic Toolbox in MATLAB®. The results of the data analysis were used to determine the health condition of the network element. A prototype of the system was implemented in a simple case scenario but we expect the system to perform efficiently in a larger complex network. The result of the simple case scenario is presented.

Keywords: *Fuzzy logic, Lightweight agents, Network health monitor, Data analyzer, communication networks, Maintenance*

1. INTRODUCTION

Maintenance is an engineering practice which involves series of activities necessary to conserve as much as possible the optimum functionalities of equipment in the process of aging. This practice is a necessary act in manufacturing outfits but it is very much important in communication network (Fernandez and Marquez, 2012), where an hour downtime may lead to a great misfortune for a company and may even be lethal for those whose lives depends on life saving devices hooked to the network (Infonetics,2006). Communication equipment (like any other equipment) usage leads to components wear and tear which invariably permits vibrations and thus reduces the original operability of the equipment. This grateful degradation of equipment can lead to total collapse of the equipment, which consequently leads to network outage if corrective measures are not timely implemented. Thus, it becomes very important in network maintenance activities to collect status information of major components of communication equipment as parameters for scheduling maintenance. This form of maintenance is referred to as proactive or predictive maintenance (Li and Lan, 2007). This maintenance practice pre-empt possibility of equipment failure, and find possible solution or report the impending outage to the network administrator timely. Proactive maintenance unlike run-to-failure maintenance uses available status data to take preventive actions before the occurrence of failure. This form of maintenance which monitors the health of communication equipment components (strahonja and Saletovic, 2007) must be an essential feature of any communication outfit that will be successful in this competitive modern ubiquitous network. The company must be able to plan better for the future, and be proactive in its maintenance and repair operations so as to meet the minimum quality of service required by the end users. It is obvious, that faults are unavoidable in communication network, timely detection and isolation is very important for network reliability, availability and robustness. In large communication network, automating maintenance practice is very crucial (Steinder and Sethi, 2004).

Until recently, most network maintenance operations relied mainly on the knowledge and expertise of human operator which is mainly corrective maintenance. This form of maintenance operation cannot cope with the modern data communication network. Computer networks is increasingly becoming more complex with impressive growth in developing countries, as the modern trend moves from Broadband Integrated Service Digital Network (BISDN) to Multi-Protocol Label Switching (MPLS) networks, thus the complexity and growth require a maintenance facility that will that will support network availability . Computer network is greatly influencing almost every human aspect of life. The advent of social networks, where long strained relationships are re-united and friendships are made is fueling the use of computer networks. In manufacturing, education, health and financial institutions, etc. the use of computer network cannot be under estimated, if any establishment is will survive 21st century challenges. As useful as the computer network is to our daily activities either at office or home, it is noted that the present telecommunication networks are usually conglomerates of many heterogeneous, very often incompatible, multi-vendor components which are very difficult to manage (White et al., 1999). The enormous increase in the size and complexity of these communication networks calls for increase in research for intelligent network management systems.

It may become too expensive for any network administrator in this region to fully rely on run-to-failure mod of maintenance. Definitely, most equipment failures give some warnings before they actually occur. The strategy for network communication administrator needs is a way to head off a catastrophic failure before it has a chance to happen. The solution lies in a technology called Predictive Condition Monitoring (PCM). With a PCM system, a problem such as warn-out parts can be picked-up by vibration and temperature sensor agents to avoid a system shutdown. Specifically, disk warn out information, disk speed and processor temperature can indicate the degree of usage of a node on computer network, these information can be used to determine the reliability of the system and when to embark on maintenance practice. The repairs can be scheduled at a reasonable time to minimize downtime and loss of revenue. With predictive maintenance, the health condition of systems components on communication network can be monitored to reduce the risk associated with downtime.

In this paper, we provide a modest scheme for predictive maintenance on communication network, mainly for critical systems in the tropical regions of the world where excessive heat aggravates system performance which may lead to failure or hardware crashes. The main objective of this work is to improve efficiency, reliability and availability of critical systems such as microprocessor based life saving devices in the hospitals, commercial web server, etc. particularly in tropical regions where excessive temperature, which the system coolant may not be able to support will affect the performance of critical systems which may lead to performance dwindling of the system or total failure/crashes of such system (Hongjun and Bara,

2001). The model combines effectiveness with reasonable cost, it is a simplified model which makes it easy to implement, we are sure it works well in the modern network which is often conglomerate of heterogonous network elements. The agents employed for collecting network elements status information have a negligible impact on available bandwidth on the network (Olajubu et al., 2008 and Valliyammai et al., 2011). Although network failures are ultimately unavoidable, intelligent fault management systems with its central component as fault detection and isolation (FDI), will help to quickly detect faults and initiate recovery mechanisms for network elements. This makes networks more robust and reliable, ultimately increasing the level of their quality of service (QoS) (Lu, 2005). We have used temperature as the main factor in this system due to susceptibility of electronic materials to excessive heat, which is common in tropical regions. LAN, inoperability due to hard disk crashes and processor failures due to excessive heat and high humidity are common experience (Soila and Narasimhan, 2005). The collected information is fed into a system Data Analyzer (DA) which analyzes the collected information and advice the network administrator on the condition of the network element. The modern fault management of today should have autonomous response and reconfiguration in the presence of unforeseen problems (faults) so as to provide a satisfactory service.

The remaining part of this paper is organized as follows; the next section discuses maintenance practices available in the industry while section 3 presents relevant work in proactive fault management on computer network. Section 4 focuses on the theory of fuzzy logic as basis for this work. The system architecture consists of NHM agents, data analyzer, and fault detector subsystem among many other components was discussed in section 5 while section 6 demonstrates the results of our prototype implementation. Finally, section 6 concludes the paper.

2. MAINTENANCE PRACTICE

Generally, maintenance involves putting faulty equipment in a proper working condition or retaining/restoring the working functionality of the equipment to optimum performance. It may include activities such as testing, measurement, replacement, adjustment and or repair etc. (Dennis, 2003).

According to Dennis (2005) maintenance practice in the industry can be broadly divided into three classes: (i) Corrective or run-to-failure maintenance, which aims at correction after equipment failure has occurred (ii) Time-directed or preventive maintenance, maintenance practices are tied to a period of time, it may be monthly, quarterly, etc. and (iii) Condition-directed or proactive maintenance, it ties maintenance practice with equipment usage.

2.1. Corrective Maintenance:

This form of maintenance happens when equipment has failed, the machine is open up to identify the component(s) that has failed or malfunctioning with the intension to repair or replace the component(s). This maintenance has no time interval; maintenance is due when the machine has failed. It is highly unpredictable and loss of revenue attached to machine failure is enormous. The main goal of corrective maintenance is to restore the normal functionality of the system within the shortest possible time and make the system available for use Gary et al., 2004). There are three phases to corrective maintenance:

i. Localization of the fault: The maintenance crew must locate the failed component within a specified period of time.
ii. Restoration of the equipment: After the maintenance crew has identified the failed component, action should be initiated to either repair or replace the faulty components.
iii. Testing the repaired or replaced system: It important that maintenance crew verify the performance of the system.

2.2. Preventive Maintenance:

Preventive or time-directed maintenance tasks are strict to maintenance scheduled tasks from time to time based on the operating age of the equipment (Yang, 2008). Scheduling preventive (that is, routine or planned) maintenance involves specifying periods at which manpower is to be allocated to an overhaul of a major functional element or group of elements of equipment. This maintenance planned action does not require any detailed information regarding the present condition of the equipment. It can help in extending the equipment life span since maintenance may be carried out before the total breakdown of the system. Although it does not indicate optimal performance of aging equipment as depreciation will affect the performance of the equipment due to wear and tear Harvey et al., 1964) yet it keeps the equipment in operation. Timed–directed maintenance does not put the usage of the equipment into consideration, in most cases, unlike run-to-failure maintenance, malfunctioning device component is often repair or replace prior to equipment failure, in order to promote continuous serviceability of the equipment.

In carrying out this maintenance practice, the past history of the equipment is often taken into consideration. The maintenance scheduled is normally based on the past observation and the behavior of the equipment. It has been shown that cost is major factor in time-directed maintenance (strahonja and Saletovic, 2007). Other factors (risk, reliability, etc.) that can influence it are still function of cost. The higher the cost the more time the organization will like to carry out maintenance activity. In telecommunication and manufacturing environment, it cost saving when maintenance is timely than when there is total breakdown or failure had occur.

2.3. Proactive or Condition-directed maintenance:

Condition-directed maintenance employs periodic monitoring of the health of equipment's vital component to forecast the overall health of the equipment. The overall health of equipment at a time is a function of the condition of all components that are vital to the functionality of the equipment. It is necessary to take caution when applying condition-directed maintenance because not all equipment components can easily be monitored. It will be an appropriate measure if condition-directed maintenance and time-directed maintenance are fused together for use so that the hybrid form will take the good advantage of the maintenance types.

Obviously, the legacy maintenance (run-to-failure) or time-directed maintenance practices can no longer cope with the 21st century communication networks or industrial environment, due to its huge loss of revenue by unplanned downtime. The communication industry is turning around to look for an effective method of maintenance which hitherto was not a concern to the industry (strahonja and Saletovic, 2007). The reason for this is very clear, an hour of LAN downtime, company may lose revenue of about million of US Dollars (Infonetics, 2006 and Chunxiao et al., 2003). It has also been shown by (Jacob, 2009, Petet Narasimhan, 2005 and Hellerstein et al., 2001) that companies that rely heavily on communication network for their operation could lose as much as hundreds of thousands U.S. Dollars for an hour of LAN inoperability. Therefore a better maintenance scheme is necessary for communication network availability.

3. COMMUNICATION NETWORKS FAULT MANAGEMENT SYSTEMS

Existing works reveal various schemes developed to solve the complexity of finding faults and isolating them on communication network. Early 1980s witnessed computer network fault management fully based on human operator equipped only with consoles to display network elements status information (Hongun and Baras, 2001). Predictive detection is often used in exploring possibility of system failure. For example, a model (Hellerstein et al., 2001) has been presented for online prediction of threshold violations in web server. The prediction addressed two major issues, the probability that the

threshold will be breached and the time frame for which the anticipated violation is likely going to occur. In this model, discrete Kalman Filter with analysis of variance was applied to get rid of non-stationaries in the system. The threshold probability violation of the system was determined using the second order autoregressive model together with change-point detection estimation. The evaluation of the system was done through simulation experiments. Experimental results presented showed that, for small times horizon value, there was reasonable prediction through time-series modeling. This technique provides tangible information when the observed value deviate from the threshold value.

For critical-mission systems like web server, where high availability is required for frequent access by the end users, preventive failover technique (Pertet and Narasimham, 2004 and Liand Lan, 2007) has been used to support high level of availability. The technique automatically switches over to a reserve system in view of unexpected failure of the server. Distributed systems have integrated replication technology with failure prediction to offer fault tolerant. The system has the predicting mechanism with some level of confidence, when a fault/failure is imminent and a set of actions to compensate for the failure event before manifestation.

More often than not, status information collected from components of network element plays a crucial role in determining the performance degradation of network elements. This information also is very useful for scheduling maintenance activities on the network. The ITU/CCITT recommended that such historical data should be retained for minimum of twelfth months to watch for persistent performance degradation (ITU/CCITT, 2006). The ITU/CCITT recommendation for preventive maintenance consists of a supervision process for anomalies, the defect supervisory process and the malfunction supervisory process. Whether it employs statistical or analytical method of fault correlation, it should cover all three concurrent levels of supervision. When threshold violation are detected early in systems, it offers a very useful information to plan to isolate such systems and timely schedule proactive maintenance. This can be achieved by using means for data gathering, we have used lightweight agents for simplicity and effectiveness. Mobile agent is known to be very useful in bandwidth usage optimization (Olajubu et al, 2008 and Valliyammai et al., 2011).

The major effort of the second generation network management systems is to integrate artificial intelligence (AI) techniques into network management systems. Means of adding intelligent components within network management framework has largely been the focus of many AI researchers. Ibrahiem and Adanan(2005) proposed a time series based expert system for fault management on computer network. The objective of using time series is to observe or model the existing data to enable future unknown data values to be forecasted accurately. Exponential weighted moving average was used for data model. The major weakness of the approach is that the expert systems cannot accurately implement the captured knowledge. Therefore, the rules in the inference engine are not fully useful to the system which makes any network that implements it to be very prone to network failures. A belief network was used to tackle the problem of fault management on computer networks. Fault propagation modeling approach adopted in this work uses a layered non-deterministic dependency graph as a system model, which is mapped into a probabilistic causality graph. The fault localization algorithms adopted for the work is bucket elimination proposed by Steinder Sethic, 2004). The bucket elimination algorithm for computing most probable explains (MPE) is exact and always outputs a solution; this informed the authors adopting the algorithms. The iterative belief propagation utilizes a message passing schema in which the belief network nodes exchange coding messages. The fault localization algorithm starts with a belief network which has evidence to zero, and all other nodes are insignificant. The algorithm proceeds in an event-driven manner, after every symptom observation applying iteration of belief updating traversing the graph according to some order. For every symptom, a different ordering was defined that is equivalent to the breadth first-order standard from the node representing the observed symptom. This work further examines the use of end-to-end diagnosis of service failures. A fault propagation model for end-to-end service failure diagnosis is a bipartite belief network in which nodes without parent (called linked nodes) represent host-to-host service failures and childless nodes (called path nodes) represent end-to-end service failure. For this model to be built, the knowledge of the logical network topology is often required. When the logical topology corresponds to the physical one, the relationships between end-to-end and host-to-host services will be obtained by analyzing the physical network connectivity. This requirement makes this model complex for easy implementation in real-life networks. The decision tree learning approach to diagnosing failures in large Internet sites (Dechter, 19996) has been proposed by Chen et al. In this work, the run time property of each request was taken and data mining and automated machine learning algorithms were employed to identify the root causes of failure. The decision trees were trained to trace user visible failures from the time the failure became apparent. Paths through the tree are ranked according to their degree of correlation with failure and node is merged according to the observed partial order of system components. The technique was evaluated using actual failures from eBay. It was discovered that algorithm successfully identified 13 out of 14 true causes of failure among hundreds of potential causes. This work goes further to justify the need for automating diagnosis systems. Likewise, researchers have employed pattern recognition techniques to estimate possibility of software failure (Li and Lan, 2007). The Hidden Markov model was used to account for interrelationship among failures; this allows the probabilities of unknown failures to be estimated based on the current events. The use of proactive maintenance is not limited to computer network alone, for instance, the scheme has been applied to the maintenance of oil mill in the food industry (Ismail et al., 2009). A probabilistic model for fault prediction in cellular network systems (Kogeda et al., 2007) has been proposed. The model used Bayesian network which is a directed acyclic graph. In the graph, each node represents a random variable to which conditional probabilities are linked given all the possible combinations of values of variable represented by the preceding nodes. Likewise, a neural network model for proactive fault detection in optical network is presented in (Arunachalam and Rajamani, 2011). The agents in the model can seamlessly sniff fault based on the information gather on each node, to predict fault and proactively re-route traffic through alternative route when impending fault is suspected on a node. Model intelligent agent was used in Kogeda and Agbinya, 2007) to timely predict and proactively arrest impending downtime of a node or entire network.

4. THE THEORY OF FUZZY LOGIC

Theory of fuzzy logic (FL) with its practical implications was first coined by Lotfi A. Zadeh in 1965 Mendel, 1995). The concept was based on the extension of the traditional Boolean logic. Fuzzy logic is a multi-valued logic that allows intermediate values to be defined between conventional evaluations such as yes/no, true/false, cold/hot, white/black etc. Concepts like "rather warm" or "pretty cold" can be expressed mathematically and implemented by computer systems, thus providing an easy means of applying a human way of reasoning to the programming of computer systems (Kaufimann, 1995; Odejobi, 2007 and Wang and Lui, 2008). Fuzzy logic systems use rules inform of "if ...then" that transforms inputs to outputs. The versatility and uniqueness of fuzzy logic is underscored in that it is able to simultaneously handle numerical data and linguistic variables (Mendel, 1995). A linguistic variable is a quintuple (X, T(X), U, G, M,), where X is the name of the variable, T(X) is the term set, i.e. the set of names of linguistic values of X, U is the universe of discourse, G is the grammar to generate the names and M is a set of semantic rules for associating each X with its meaning.

According to Kanfimann (1995), the classical set theory states that, the set A is defined by a characteristic function $\mu_A(x)$, it maps elements of A to {0,1} so that for $x \in A$

$$\mu_A(x) = 1, if x \in A \text{ and } 0, if x \notin A \quad (1)$$

Therefore, for every element of x of A $\mu_A(x) = 1$, if $\mu_A(x) = 0$ then x is not an element of A. Between 1 and 0, there is a gap, which consists of the membership grades, it is these membership grades that produce the membership function which assigns to each object a grade of membership which is associated with each fuzzy set. When the membership grade of an object is 1, it implies the object is absolutely in the set. But when the membership grade is 0 it means the object is absolutely not in the set. The in-between cases are assigned values between 0and1. Thus, the fuzzy set theory specified that a set A is defined by a membership function $\mu_A(x)$ which maps elements of A to {0, 1} so that

$$\mu_A = 1, \text{ if } x \in A$$
$$= 0, \text{ if } x \notin A \quad (2)$$
$$= 0 < \mu_A < 1$$

(x is a member of A with a membership degree of μ_A)

The membership function which decides the characteristics of the fuzzy subset A is given as:

$$A = \sum_{i=1}^{n} \frac{\mu_A(x_i)}{x_i} \quad (3)$$

Equation (3) is the general mathematical expression of fuzzy subset A of x where x is the whole data set often referred to as universe of discourse. In a finite fuzzy set, the universe of discourse is often divided into several regions which belong to different predicates.

$X = (x_1, x_2, x_3, \ldots\ldots\ldots\ldots, x_n)$

In the recent years, fuzzy logic as modeling tool is gaining the attention of many researchers especially in Science and Engineering. This is because complex systems are easily modeled using fuzzy logic. Many systems such as food processing (Odejobi, 2007); Robot navigation (Wang and Lui, 2008); Diagnosis (Hooshmand and Banejad, 2006); etc have been molded using fuzzy system. Other applications in the area of fault prediction are equipment failure prediction (Ogunjobi and Ajayi, 2003); fault detection in fluid system (White and Lakay, 2008). More specifically, computer network-centric applications have received significant touched by fuzzy application. Ramirez et al. (Ramirez et al., 2006) modeled traffic control on computer network using fuzzy logic while Revathi et al.Revathi et al., (2006) applied fuzzy logic to congestion control in differentiated service network; Fang and Li (Feng and Minqiang, 2011) handled risk management in information system; in the same way Su et al. Ing-Jiunn et al., (2012) applied fuzzy system to area temperature monitoring in wireless networks. To the best of our knowledge, fuzzy logic system is yet to be applied to hardware fault prediction on computer network.

5. FAULT DIAGNOSIS ARCHITECTURE

The system architecture represents the different modules and the interaction among them in Fig. 1 while Fig. 2 presents the system class diagram.

The following classes of lightweight agents are found on the system:

5.1. Network Health Monitor (NHM)

The Network Health Monitor (NHM) houses individual group of agents that migrate to the network to examine the health (condition) of specific components of network elements especially critical servers and switches. The data acquisition is done through all the tiny agents that monitor the status of network elements components. Status information of network elements are collected through sensors attached to the components of critical servers or switches on communication network. The data collected from these components by the agent are assumed to be quantitatively discrete. For the purpose of this work, three important components are considered. The agents submit the collected status information in a discrete form to the Data Analyzer subsystem along with the name of the network element.

5.1.1. *Hard disk health sensor (HDDss)*

The agent uses the spinning speed and temperature of the hard disk to determine the present health of the system. The hard disk remains the only storage medium for either of the computer system or the network resources. It is the hard disk that accommodates the necessary protocols for communication, operating systems, software drivers, etc. If the hard disk crashes, the whole network is put to a halt. Therefore, it is necessary that the health condition of the hard drives on communication network be monitored to forestall any sudden crashes of the network. There are many reasons why hard drives get damaged; overheating is probably the most common factor. The spinning of the hard disk which is about a thousand revolutions per minute generates great heat. The larger and faster the hard disk, the more it generates heat. Thus, it is liable to damage easily, especially when the system is on communication network that can be busy for several days nonstop. The temperature plays a major role in the usefulness of hard disk. Abnormally high temperatures can lead to data loss on the storage device and if the temperature goes too high, the device may crash. The recommended temperature for hard disk ranges from 35°C to 40°C. If the temperature rises by 10°C, the durability and the efficiency of the device becomes two times less than its original quality.

5.1.2. *Processor health sensor (PROss)*

Excessive heat damages electronics. Monitoring the temperature of CPU will help keep the processor running properly. When a processor temperature rises beyond normal, the computational power is reduced and this can be followed by the system "hanging". Any rise above this point may lead to processor crash. To proactively forestall this problem, the PROss interact with processor through a sensor to know the temperature range and use this information to determine the type of problem that are likely going to occur. It is very obvious that processors on grid are engaged in long time execution which generates a lot of heat; this is why they are very prone to crashes. Proactive monitoring of the health of the processor can help keep the processor viable for a long time.

5.1.3. *RAM health sensor (RAMss)*

The Random Access Memory (RAM) is a very important organ in the communication network component; all the communication facilities and supportive systems must be loaded and run in the memory which is RAM. Therefore, RAM is another component on the system whose malfunctioning could result in network outage if not properly monitored. As temperature affects the other components, excessive temperature can also affect the performance of RAM. The RAMss sense the temperature of the RAM and the likely effects.

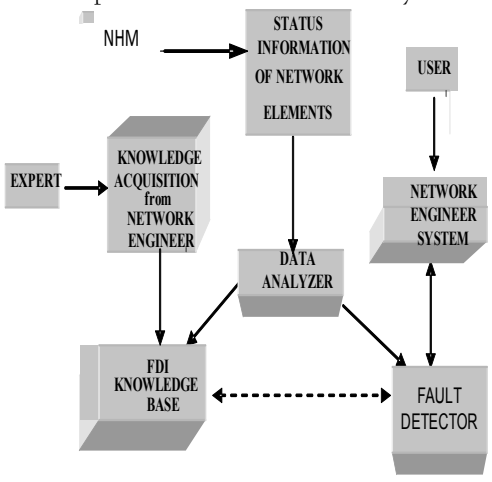


Fig.1: System Architecture

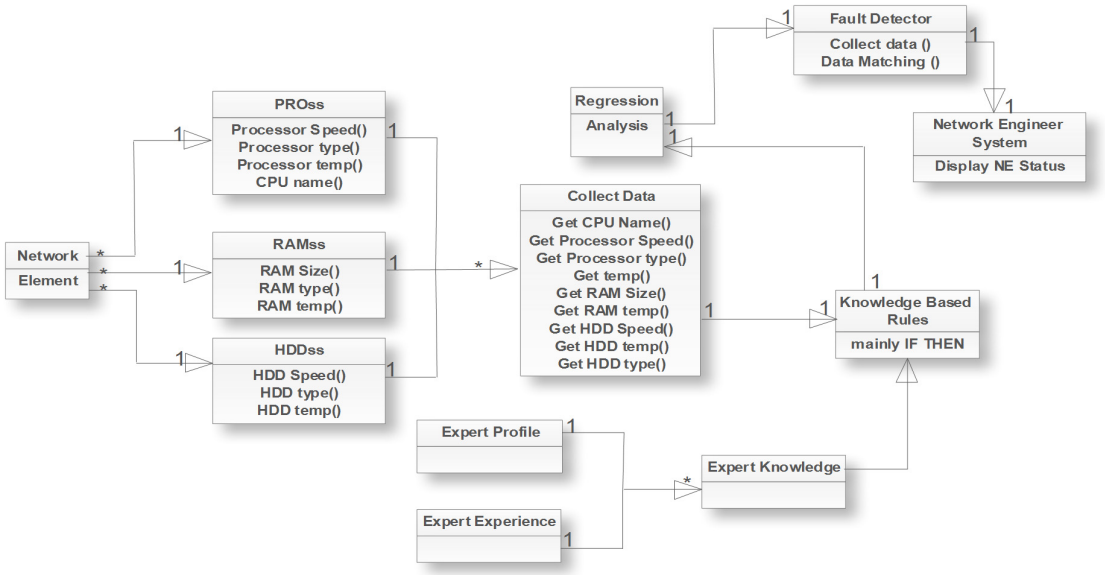


Fig. 2: The system Class diagram

5.2. Data Analyzer (DA)

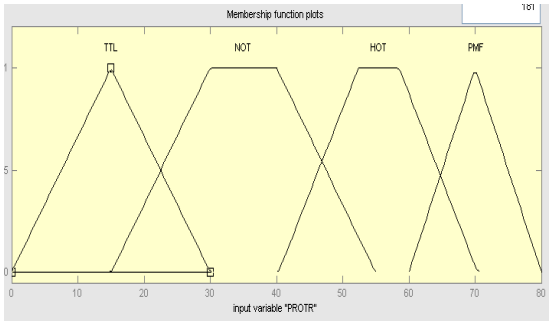
The DA is the subsystem that coordinates and analyzes the various data that are submitted by the network health sensors. The DA is modeled using fuzzy logic Toolbox available in MATLAB®.

The data used for the fuzzy logic model in this research were collected from the data sheet of different vendors of system components. Our limitation is that the model cannot take care of all vendors' products but this were showcase to encourage predictive maintenance work on communication network rather than the traditional maintenance work. The data for each component were fuzzified for easy implementation in fuzzy logic system. The DA fuzzy logic system has five inputs which are: (i) Random Access Memory Temperature (RAMT), (ii) Hard Disk Temperature Range (HDDTR), (iii) Hard Disk Rotation Speed (HDDRS), (iv) Processor Temperature Range (PROTR), and (v) Processor Speed (PROSR). System Degree of Failure (SYSDF) which indicates the present condition of the system is single output of the system. Table 1 gives the data fuzzification for the system. The data fuzzification converts each unit of input data to a degree of membership by a call on some membership function $\mu_{(x)}$ within the universe of discourse. In the process of data fuzzification, each input data is mapped with the conditions of the rules to establish the degree of fitness on how each rule matches the particular input. The fuzzified data were used to generate the membership function for the DA as shown in Fig. 3 (a: RAM Temperature, b: HDD temperature and c: processor temperature). As shown in Table 1, our system has five input variables (i.e. RAMT, HDDTR, HDDRS, PROTR and PROSR) and one output variable (i.e Probability of Green Light (PGL)).

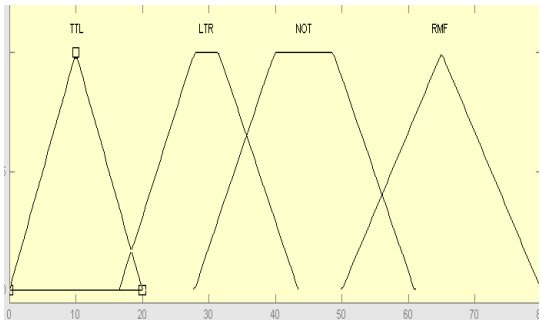
We experimented with different type of membership functions and using the result of our experiment and our experience of the characteristics of the fault identification and isolation on communication network, we selected the trapezoid (*trapmf*) and the triangular (*trimf*) membership functions which have the following general equations (Equations 4&5):

$$f(x,v,w,y,z) = \max\left\{\min\left(\frac{x-v}{w-v}, 1.0, \frac{z-x}{z-y}\right)\right. \quad (4)$$

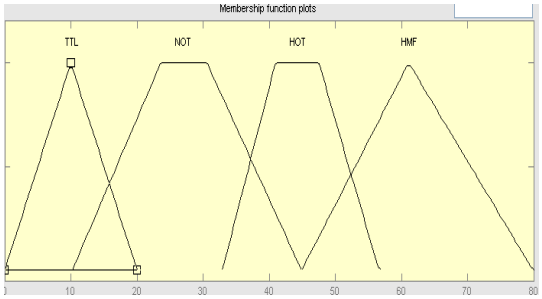
$$f(x,v,w,y,z) = \max\left\{\min\left(\frac{x-v}{w-v}, \frac{y-x}{y-z}, 0.0\right)\right. \quad (5)$$



(a)



(b)



(c)

Fig. 3: a: RAM Temperature, b: HDD temperature c: processor temperature

b

Where v, w, y and z define the co-ordinates of the triangular and trapezoidal membership functions and x is the input variable to the function. The main criteria for selecting these functions are their stability, simplicity and ease of design (Harvey et al.,1964).

The shape of the membership function is triangular and trapezoidal. This is for easy calculation of each input degree of membership function.

5.2.1. *Data Analyzer surface plot*

The surface plot for DA shows the relationship among the five inputs (RAMT, HDDTR, HDDRS, PROTR, and PROSR), when any two inputs are selected and output (SYSDF) in a 3-dimentional mesh plot. The two inputs selected for this plot are RAMT and PROTR. Fig. 3 depicts the rule implementation (viewers) in MATLAB® fuzzy logic while Fig. 4 is the result of inputs synchronization through the 56 rules in the knowledge base. It shows the influence of each of the inputs on the final output of the system. This is the three-dimensional plot of the two inputs and output.

5.3. Fault Detector Subsystem

The actual fault detection or the probability of any network failing is done by the fault detector subsystem. The results of DA become inputs for the fault detector subsystem. The subsystem matches its input with the available data at the inference engine to determine the rule that will be fired.

5.3.1. *Fault Detector Rules*

The Knowledge-base of fault detector contains about 56 rules. Fig. 4 depicts the rules implementation by MATLAB® fuzzy logic. The rules are meant to be fired to decide the condition of each component in network element that is considered in this research work. These nine samples of the rules are presented to showcase the rules in the knowledge base of the system. The rules combined all the input factors to decide the viability of the system. To properly interpret and understand the rules readers are expected to use Table 1 so as to understand the meaning of the inputs. The samples rules are presented as follows:

1 **IF** RAMT **IS** TLL **AND** HDDTR **IS** TTL **AND** HDDRS **IS** RTL **AND** PROTR **IS** TTL AND PROSR **IS** STL **THEN** SYSDF **IS** *SMLF*

2 **IF** RAMT **IS** TLL **AND** HDDTR **IS** NOT **AND** HDDRS **IS** LOR **AND** PROTR **IS** NOT **AND** PROSR **IS** LOS **THEN** SYSDF **IS** *SSNF*

3 **IF** RAMT **IS** TLL **AND** HDDTR **IS** HOT **AND** HDDRS **IS** NOT **AND** PROTR **IS** HOT **AND** PROSR IS NOS **THEN** SYSDF **IS** *SMLF*

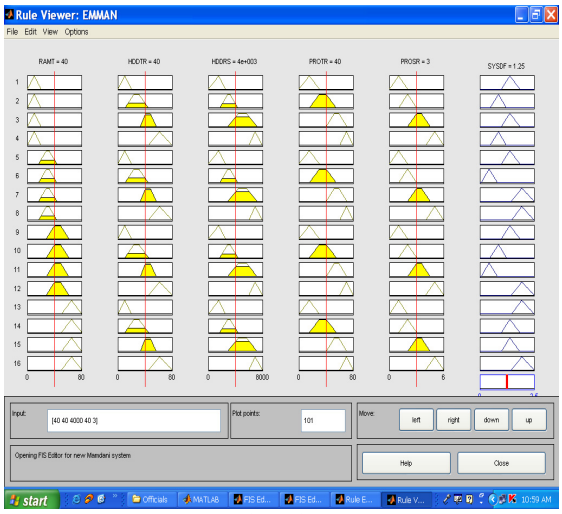


Fig. 4: Rules implementation

Table 1: Fuzzification of Input Data

F. V.	Implication	PROSR
HDD Temperature Range		
TTL	Temperature Too Low	0-20
NOT	Normal Operating Temperature	10-45
HOT	High Operating Temperature	35-55
HMF	RAM May Fail	45-80
Processor Rotation Speed		
RTL	Rotation Too Low	0-2500
LOR	Low Temperature range	1500-4500
NOR	Normal Operating Temperature	3000-7200
HMF	RAM May Fail	6000-8000
Processor speed Rotation		
STL	Rotation Too Low	0-2
LOS	Low Temperature range	1-3
NOS	Normal Operating Temperature	2-4.5
PMF	Processor May Fail	4-6
Processor Temperature Range		
TTL	Temperature Too Low	0-30
NOT	Normal Operating Temperature	15-60
HOT	High Operating Temperature	45-70
PMF	Processor May Fail	60-80
Output: System Degree of Failure		
SIGC	System In Good Condition	0.0-0.8
SSNF	System Should Not Fail	0.5-1.2
SMLF	System May Likely Fail	0.9-1.8
SMFM	System May Fail Moment	1.5-2.5

5.4. Network engineer's system (NES)

The Network Engineer's System (NES) is either the engineer laptop or desktop. This is the system where the FI sends all the faults interpretation to NES for the network engineer's immediate action. It is the colour indication against the name of the system that informs the network engineer about the present condition of the network element. When component is in a critical condition, the system gives the network engineer a time limit within which the repair/replacement must be done. As the time approaches, the system reminds the network engineer of the danger ahead if the repair/replacement is not done in time.

6. EXPERIMENT AND RESULTS DISCUSSIONS

The Fault detection subsystem is the organ that coordinates and displays the health conditions of various network elements present on the network on NES. To verify the viability of our proposed model, an ad-hoc network of ten computers were set up. The mobile agents were developed to monitor the components of the system as described in section three through sensor attached to the components. The system runs for a considerable time so as to allow some degree of stability. The data collected by the agents were processed by the DA and then channeled to fault detection subsystem. For further analysis and aggregation before displayed on NES.

After the analysis, the subsystem classifies the health conditions into four categories: (i) Normal conditional i.e. the component is working perfectly thus do not require any maintenance or repair issues, which is indicated by green colour against name of the system. (ii) Deviating condition (a condition where the element has started showing cases of dwindling performance i.e. some abnormal behavior which deviate from the standard performance but is still working well. This case is identified by pink colour. (iii) Critical condition shows the network element is at the verge of failure, which is a condition where the efficiency of a component has dropped drastically. At this point the attention of Network Engineer is required because this could result to failure and collapse of the system. This is indicated with red colour in Fig. 5. The fourth condition is the faulty condition when the element has totally packed up and is no longer functioning. This fourth condition is necessary because it is difficult to remove network outage completely but can be minimized. When the component is out of use, black colour is shown on the system. The system knows this when agents can no longer access the components' data. Thus fault detector handles fault interpretation and

the DA is implemented with fuzzy logic. Fuzzy systems are known to be very good in handling imprecise data model.

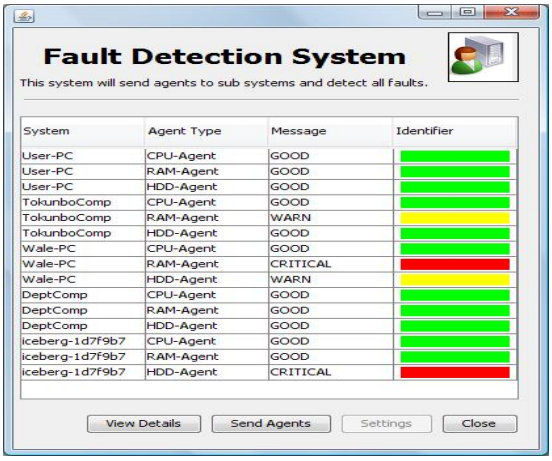


Fig. 5: Fault Detection subsystem

7. ADVANTAGE OF THE PROPOSED MODEL

Maintenace activities on communcation network are carried out to maintain network availablity, improve quality of service, and retain the confidence of end users. To attain this objectives, communication network maintenance activities should not be based on time scheduled only, which is the present mode of scheduling in many communication networks. The time based maintenance suggests that the whole or part of the network is shut down for the maintenace or system upgrading period. During this period, all end users are deprived of use of the network, putting them at a serious disadvantage especcially users that have no alternative network for communication. If maintenance or upgrading activities are handled proactively, i.e. network elements status information are used to schedule maintenance activities (replacement of components, repair, ugrading, etc.) length of time used for maintenace will greately reduced, making the network available to users. Individual network element (server, routers, etc.) will be scheduled for maintenance on the basis of usage, instead overhauling all network elments at the same time. The operational condition of the element dictates the period for maintenance rather than scheduling maintenance based on time.

8. CONCLUSION

In this paper, we have developed a system that assists network administrator to discharge his duty with ease. The system used status information of different components of a system collected by tiny agents to determine the health condition of the whole system. The data collected is analyzed by fuzzy logic model developed to predict the viability of the system. The condition of each network element is displayed at the network engineers system. This model forms the basis for scheduling a proactive maintenance scheme on communication network.

We have essentially concentrated our effort on hardware faults in this paper; we hope to continue on some other issues (network congestion, software faults, link failures, etc.) on communication network in the future research work.

REFERENCE

Arunachalam M. and Rajamani V. (2011): Distributed Fault Detection and Localization Algorithm using Artificial Neural Network in Optical WDM Networks. European Journal of Scientific Research 56 (2): 194-203.

Chunxiao Chigan, Gary W. Atkinson, and Ramesh Nagarajan (2003): Cost Effectiveness of Joint Multilayer Protection in Packet-Over-Optical Networks. Journal of Lightwave Technology, 21(11): 2694-2704.

Dechter R. (1996): Bucket Elimination: A Unifying Framework for Probabilistic Inference. In Uncertainty in Artificial Intelligence, E. Horvitz and F.V. Jensen Eds., San Mateo, C.A.: Morgan Kaufmann, pp. 211-219

Dennis H. Shreve (2003): Integrated Condition Monitoring Technologies A Technical Report at IRD® Balancing LLC.

Feng Nan and Li Minqiang(2011): An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 11(7): 4332-4340.

Fernández Gómez J. F. and Crespo Márquez, A. (2012): Maintenance Management in Network Utilities, Springer Series in Reliability Engineering, Springer-Verlag London.

Hellerstein J. Zhang F., Shahabuddin P., (2001): A Statistical approach to predictive detection . Computer networks. Internal Journal Of Computer and Telecomminucations Networking pg. 77-95.

Hongjun and Baras, (2001): A Framework for Supporting Intelligent Fault and Performance Management for Communication Networks. In: Proceedings of IFIP/IEEE International Conference on Management of Multimedia Networks and Services (MMNS 2001) pp. 227-240.

Gary Warren, Notle Ronald, Funk Ken, and Merrell Brain (2004): Network simulation enhancing network management in real-time. ACM Transactions on Modeling and Computer Simulation, 14(2): 196-210.

Harvey m. Wagner, Richard j. Giglio, and R. George Glaser (1964): Preventive Maintenance Scheduling by Mathematical Programming. Management Science 10(2):316-334.

Hooshmand, R., & Banejad, M. (2006): Application of fuzzy logic in fault diagnosis in transformers using dissolved gas based on different standards. In: Proceedings of World academy of science, engineering and technology Vol. 17, pp. 151–161.

Ibrahiem and Adanan(2005): Fault Detection of Computer Communications Networks Using an Expert System - American Journal of Applied Sciences, 2 (10): 1407-1411.

Infonetics. (2006): The Costs of Enterprise Downtime: North American Vertical Markets available at http://www.optrics.com/emprisa_networks/2006_UPNA05_DWN ToC_Ex cerpts.pdf [15th, March 2007].

Ing-Jiunn Su, Chia-Chih Tsai, and Wen-Tsai Sung (2012): Area temperature system monitoring and computing based on adaptive fuzzy logic in wireless sensor Network. Applied Soft Computing, 12(5): 1532-1541.

Ismail A. R., Ismail R., Zulkifli R., N. K. Makhtar and B. M. Deros (2009): A Study on Implementation of Preventive Maintenance Programme at Malaysia Palm Oil Mill. European Journal of Scientific Research 29(1): 126-135.

Jacob Jackson (2009): The high cost of failure on the network. Available at http://gcn.com/articles/2009/10/26/numerator-cost-of-failure.aspx [15th June 15, 2012].

Kaufimann A. (1995): Introduction to the Theory of Fuzzy Subsets.I : Fundamental Theoretical Elements Academic Press Inc. 1975.

Kodega Okuthe P., Agbinya Johnson I. and Christian W. Omli (2007): A Probabilistic Approach To Faults Prediction in Cellular Networks. Proceedings of the Fifth International Conference on Networking. Pp 130-135.

Kogeda Okuthe P. and Agbinya Johnson I. (2007): Proactive Cellular Network Faults Prediction through Mobile Intelligent Agent Technology. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications pp 55-60.

Li Y. and Lan Z. (2007): Current Research and Practice in Proactive Fault Management. International Journal of Computer and Applications. 29(4): 408-412.

Lu Yang (2005): Improving Network Maintenance for Higher Quality of Service. China Communication August, 2005 pg 12-13.

Mendel J.M.(1995): Fuzzy Logic for Engineering: A Tutorial Proceedings of the IEEE .83 (3): 345-377.

Odejobi, O. A. (2007). Computational modeling of systems engineering: A case study of the cassava processing plant. Journal of Computer Science & Its Applications,14(2): 1–9.

Ogunjobi A. O. and Ajayi O.A. (2003): Failure Prediction and Reliability Analysis of Equipment using Fuzzy Logic. *Nigerian Journal of Mechanical Engineering*, 1 (1): 75-84.

Olajubu E. A., Aderounmu G.A. and Adagunodo E. R. (2008): Optimizing Bandwidth usage and Response Time using Lightweight Agents on Data Communication Network. T. Sobh et al. (eds), Novel

Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics, (ISBN:978-1-4020-8736-3) Springer Science+Business Media B.V.\Netherlands. pg. 335-340.

Pertet, Soila and Narasimhan, Priya (2005): Causes of Failure in Web Applications. A Technical Report No: CMU-PDL-05-109. Parallel Data Laboratory Carnegie Mellon UNiversity.

Pertet S.and Narasimham P. (2004): Proactive recovery in distributed CORBA applications, Proceedings of International Conference on Dependable systems and Network. Pg. 357-366.

Ramirez K., Alanis A., Castillo O., Arias H., and Melin P (2006): Monitoring and Diagnostics with Intelligent Agents Using Fuzzy Logic. Proceedings of the 2006 Internal Conference on Artificial Intelligence (ICAI 2006) pp. 571-577.

Revathi T., Muneesswaran K. and Ramar K. (2011): Fuzzy enabled congestion control for differentiated services network. Applied Soft Computing, 11(8): 5457-5462.

Soila M. Pertet and Priya Narasimhan (2005): Causes of Failure in web applications. Technical Report PDL-CMU-05-109, Carnegie Mellon University.

Steinder Małgorzata and Sethi Adarshpal S. (2004): A survey of fault localization techniques in computer networks. Science of Computer Programming 53 pg. 165–194.

Steinder M. and Sethic A.S. (2004): Probabilistic Fault Localization in Communication Systems Using Belief-Networks, *IEEE/ACM Transactions on Networking*, 12(5): 809-821.

Strahonja Vjeran and Saletovic Kristijan (2007): Proactive Approach to the Incident and Problem Management in Communication Networks. Journal of information and organizational sciences, 31(1): 245-259. Valliyammai.C, Thamarai Selvi.S (2011): Mobile Agent Based Automated Deployment Of Resource Monitoring Service In Grid. Ubiquitous Computing and Communication Journal 6(2): 786-790.

Wang, M., & Lui, J. N. K. (2008): Fuzzy logic-based real-time robot navigation in unknown environment with dead ends. Robotics and Autonomous Systems, 56(7), 625–643.

White Christopher J. and Lakay Heba (2008): A fuzzy inference system for fault detection and isolation: Application to a fluid system. Expert systems with Applications 35(3): 1021-1033.

White T., Bieszczad A., and Pagurek B. (1999): "Distributed Fault Location in Networks Using Mobile Agents": In the Proceedings of the Second International Workshop on Intelligent Agents for Telecommunication Application. Paris, France, pp. 130-141.

Yang Liu (2008) Predictive Modeling for Intelligent Maintenance In Complex Semiconductor Manufacturing Processes. A PhD Thesis submitted at Department of Mechanical Engineering, University of Michigan, USA.

ITU/CCIT (2006): Maintenance Philosophy for Telecommunication Networks, ITU/CCITT Recommendation M.20, 1992.